IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
DANVILLE DIVISION

IN THE MATTER OF THE SEARCHES OF **242 HENRY STREET, STANLEYTOWN VIRGINIA 24168, TO INCLUDE CURTILAGE AND OUTBUILDING/VEHICLES ON THE CURTILAGE OF THE PROPERTY.**	)	**FILED UNDER SEAL** Case No. 4-24-mj-2

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Bailey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises, outbuildings, and curtilage of the location known as 242 Henry Street, Stanleytown, Virginia ("TARGET ADDRESS") located in Henry County, Virginia which is located within the Western District of Virginia and further described in Attachment A, for the things described in Attachment B.

2. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and make arrest for, the offenses enumerated in Titles 18, 19, 21, 31 of the United States Code and other related offenses, since 2017.

3. I am a Task Force Officer with the Drug Enforcement Administration (DEA) and have been since 2017. I am also a Detective with the Lynchburg Police Department (Virginia) and have been so employed since 2002. I am currently assigned to investigate drug trafficking

organizations as a member of the DEA, Washington Field Division/Roanoke Resident Office. My duties as a Task Force Officer involve the investigation of various criminal activities of narcotics traffickers and their associates. In investigating these matters, I have acted as a case agent, an undercover agent, and a contact agent for confidential sources. These investigations have resulted in the issuance of federal search warrants, seizure warrants, indictments, and convictions of persons for federal narcotics violations. During my employment as a law enforcement officer, I have received multiple hours of training in narcotics enforcement and investigative techniques, and I have personally participated in numerous investigations. I have also spoken on numerous occasions with informants, suspects, and other experienced narcotics traffickers concerning the methods and practices of drug traffickers, including the methods and practices used by traffickers of methamphetamine, heroin, and cocaine. I have been involved in the execution of numerous search warrants on electronic devices, including cellphones, and in obtaining location information for those devices.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses which I have found to be reliable. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Quinn HAIRSTON ("HAIRSTON") and others, are engaged in a conspiracy to violate federal drug laws, specifically: narcotics trafficking, in violation of 21 U.S.C. § 841(a); offenses involving the use of communications facilities in commission of narcotic offenses, in violation of 21 U.S.C. § 843(b); and maintaining a drug-involved premises, in violation of Title 21, United States Code, Section 856. There is probable cause to search the locations described in

Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

6. The TARGET ADDRESS is a residence located at 242 Henry Street, Stanleytown, Virginia 24168. That residence is described as a gray colored, single story, vinyl sided, single family residence. The TARGET ADDRESS contains a shed/outbuilding on the property. The TARGET ADDRESS is believed to the residence of Quinn HAIRSTON and where he resides most often.

PROBABLE CAUSE

Identification of Quinn HAIRSTON as a Narcotic Distributor

7. The United States, including Drug Enforcement Administration ("DEA"), Bureau of Alcohol, Tobacco, Firearms, and Explosive ("ATF"), Henry County Sheriff's Office ("HCSO") and the Lynchburg Police Department ("LPD"), are conducting a criminal investigation of Quinn HAIRSTON and others regarding violations of distribution and possession with intent to distribute methamphetamine and other controlled substances, in violation of 21 U.S.C. § 841(a)(1), and conspiracy to distribute methamphetamine and other controlled substances, in violation of 21 U.S.C. § 846, in the Western District of Virginia and elsewhere.

8. HAIRSTON has been identified by a cooperating defendant ("CD-1") as a source of supply of cocaine, marijuana, and fentanyl. HAIRSTON's home residence was identified as 242 Henry Street, Stanleytown, VA 24168 ("TARGET ADDRESS"). HAIRSTON was previously convicted of felony offenses, including convictions for Malicious Wounding,

Unlawful Possession of a Firearm, and Possessing a Controlled I/II Substance. HAIRSTON is pending trial in Martinsville, Virginia for multiple counts of Distribution of Cocaine.

9. CD-1 is a convicted felon who is a registered confidential reliable informant with the Lynchburg Police Department. CD-1's criminal conduct includes, but is not limited to, convictions for larceny, forgery, assault, and narcotic offenses. Law enforcement apprehended CD-1 with narcotic distribution and firearm related offenses in the winter of 2023, and, for potential consideration towards the disposition of his/her crimes, CD-1 began cooperating with law enforcement. While CD-1's track record and criminal history are significant, law enforcement is unaware of any false or misleading information provided by CD-1 during his/her cooperation with law enforcement. Law enforcement has found CD-1's information to be truthful and reliable. CD-1 has conducted a controlled purchases of illicit narcotics under the direction and supervision of law enforcement. CD-1 has provided information that has been corroborated through law enforcement's independent investigation and information received from other Confidential Sources.

10. On or about January 29, 2024, at the direction of law enforcement, CD-1 contacted HAIRSTON and inquired about the availability of illicit narcotics. HAIRSTON quoted CD-1 a price of a kilogram of cocaine for $22,000 and fentanyl pills for $3/each. HAIRSTON advised he only sold fentanyl pills by the packs of 1,000.

11. CD-1 advised HAIRSTON that he/she wanted to purchase 2,000 fentanyl pills from HAIRSTON. HAIRSTON agreed to meet CD-1 on the evening of January 30, 2024 in Lynchburg, VA to facilitate that transaction. HAIRSTON advised that he was already in possession of the fentanyl pills.

12. On January 30, 2024, law enforcement located a vehicle, being rented by HAIRSTON, travelling south through Amherst County in the direction of Lynchburg, VA. That vehicle was seen being operated by a black male. HAIRSTON's operator's license status was checked and determined that his driver's privilege was suspended in the Commonwealth of Virginia.

13. A traffic stop was initiated on that vehicle and HAIRSTON was found to be driver and sole occupant of the vehicle.

14. A Lynchburg Police K-9 handler arrived on scene of the traffic stop and deployed his narcotic detection K-9 to conduct a free air search around the vehicle. The handler advised that the K-9 alerted to the odor of illicit narcotics coming from/about the truck.

15. A search of the vehicle was conducted and yielded a firearm in the center console (reported stolen out of Martinsville, VA) and approximately 2,000 tablets in the map pocket behind the driver seat. Those tablets field tested positive for fentanyl.

16. Law enforcement then obtain a state issued search warrant for the TARGET ADDRESS. During the search of that residence law enforcement located suspected fentanyl pills, other unknown pills, suspected crystal methamphetamine, suspected powder cocaine, digital scales, drug packaging material, and ammunition. Law enforcement also located documents in residence addressed to HAIRSTON.

17. HAIRSTON was charged in Amherst County, Virginia for Possessing Fentanyl with the Intent to Distribute and Possessing a Firearm by a Convicted Felon. HAIRSTON was held without bail at the Amherst Adult Detention Center.

18. On January 31, 2024, law enforcement monitored a phone call place by HAIRSTON from the detention center. That call was placed at 2359PM on January 30, 2024, the

day of his arrest. It should be noted that all calls placed from the facility are subject to monitoring and there is a preamble at the beginning of each call that states that. During that call, an unknown male told HAIRSTON that law enforcement had executed a search warrant on his house (TARGET ADDRESS). HAIRSTON stated, "I kind of need to know what the fuck has been moved around in there". HAIRSTON then instructed the male that he needed the male to the get the "wheels out of the shed". HAIRSTON then stated, "I don't know how the word this… is the (w)hole still together… you know what I'm talking about?" The caller advised that it was. HAIRSTON then stated, "Well… It ain't too bad then". Later on in the call, HAIRSTON asked again if the "(w)hole was still together". HAIRSTON was told that it was. HAIRSTON responded again that it wasn't "too bad" then. Lastly, during the call a female became a part of the phone call. The female advised she collected HAIRSTON's shoes and clothes from the residence.

19. During the search of the TARGET ADDRESS on January 30, 2024, law enforcement identified tires inside a shed located on the property. Law enforcement did not locate a "hole" containing narcotics or contraband, or an amount of narcotics that would be consistent with the term "whole."

20. This affiant knows through his training and experience narcotic traffickers do not speak plainly when talking about criminal activity on the phone. This affiant knows this is especially true when talking on a phone line that is being recording and possibly monitored by law enforcement. This affiant interprets HAIRSTON conversation by meaning that law enforcement possibly missed evidence of HAIRSTON's Drug Trafficking Operation during the aforementioned search warrant. This affiant believes that there could be a literal "hole" or a collective "whole" that contains evidence of this operation.

21. Law enforcement has continued surveillance on the TARGET ADDRESS and observed unknown subjects removing furniture from the property. It is unknown if those subjects were the individuals who spoke to HAIRSTON on the jail call or if they took any evidence from the TARGET ADDRESS.

Identification of and Continued Criminal Activity Associated with the TARGET ADDRESS

22. Law enforcement queried HAIRSTON through records of the Department of Motor Vehicle. Based on that query it was determined that HAIRSTON's registered home address was 242 Henry Street, Stanleytown, VA ("TARGET ADDRESS"). That address is approximately seven miles from Martinsville, VA.

23. Law enforcement queried HAIRSTON through the National Crime Information Center (NCIC) data base. Based on that query it was determined that HAIRSTON was listed as a Sexually Violent Predator. HAIRSTON's home address through the Sex Offender Registry was listed at the TARGET ADDRESS.

24. Law enforcement queried the TARGET ADDRESS through the call history data base of the Henry County Sheriff's Office (Virginia) and determined that HAIRSTON was served civil process at the TARGET ADDRESS. The TARGET ADDRESS is located within Henry County, Virginia.

25. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that Quinn HAIRSTON, and others, have violated Title 21, United States Code, Section 841, to wit: distribution of methamphetamine, fentanyl and cocaine, which are controlled substances, and that drugs, documentation, and other items related to the illegal

distribution of methamphetamine, fentanyl, and cocaine will be located in the TARGET ADDRESS.

26. Based upon my training, expertise, and experience, I know that:

a. Distributors of controlled substances and money launderers often keep ledger books, telephone books, receipts, drug/money customer lists, photographs and other papers that identify co-conspirators and their locations or residences and that relate to the importation, transportation, purchasing and distribution of controlled substances and proceeds derived from said sales;

b. Drug traffickers generate substantial profits because of drug dealing which the courts have recognized as probative evidence of crimes motivated by greed, in particular, trafficking controlled substances. Drug traffickers often place assets in corporate entities in order to avoid detection of those assets by law enforcement agencies. These assets often are placed in other person's names, even though the drug dealers continue to use these assets and exercise dominion and control over them. They also often maintain on hand large amounts of United States currency in order to operate and finance their ongoing drug business;

c. Drug traffickers commonly "front" (i.e. provide on consignment) controlled substances to their clients and the aforementioned books, records, receipts, notes, ledgers, etc. are maintained where the drug traffickers have ready access to them. It is common practice for large-scale drug dealers to conceal contraband, proceeds and drug sales and

records of drug transactions in secure locations within their residences, stash houses, and/or places of business for ready access and to conceal such items from law enforcement authorities. Persons involved in large scale drug trafficking often conceal in their residences, stash houses, and/or places of business, caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry, automobile titles and other items of value which are proceeds of drug transactions and evidence of financial transactions relating to obtaining, transferring, secreting or spending large sums of money acquired from engaging in narcotics trafficking activities;

d. When drug traffickers amass large proceeds from the sale of drugs, they often attempt to legitimize or "launder" these profits. To accomplish this, drug traffickers may utilize, but are not limited to, domestic and foreign banks and/or financial institutions and their attendant services, such as securities, cashier's checks and money drafts;

e. It is common practice for large-scale drug traffickers to travel to their source and distribution points to facilitate their trafficking. After purchasing their drugs, drug traffickers often transport or cause to be transported their drugs to areas in which they will distribute them. The methods of transportation include, but are not limited to, commercial carriers, private airplanes, ocean going motor vessels, rental or private automobiles, and government or contract mail carriers;

f. Drug traffickers commonly cause to be taken photographs of themselves,

their associates, their property and items used in the distribution of controlled substances. These traffickers usually maintain these photographs at their residences or places of business;

g. Narcotics traffickers use safes, surreptitious compartments and money counting machines to count and store the profits of their narcotics business;

h. Narcotics traffickers commonly possess at their residences, stash houses, or places of business, drugs, paraphernalia, and materials for packaging, cutting, weighing and distributing heroin, including, but not limited to scales, plastic wrap, plastic baggies, paper slips, tin foil, stamp pads, stamp ink and various cutting agents;

i. Drug traffickers commonly use electronic devices and storage components including, but not limited to, cellular telephones, computers, telex machines, facsimile machines, currency counting machines, telephone answering machines, computer software, tapes, discs, CD, DVDs, and audio tapes to store records of drug sales, ledgers, supplier's/customer's contact information, financial records, images, audio/video recordings and other related documents related to the trafficking and sale of narcotics;

27. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that U.S. Currency, documentation, and/or other items related to the illegal distribution of narcotics and money laundering further described in Attachment B will be located at the TARGET ADDRESS.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found at the TARGET ADDRESS, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium is found at the TARGET ADDRESS, there is probable cause to believe relevant records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also

keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the Crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET ADDRESS because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the Criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers

typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the Crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a Crime (e.g., internet searches indicating Criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to communicate online with a victim in a fraud scheme, the individual's computer will generally

serve both as an instrumentality for committing the Crime, and also as a storage medium for evidence of the Crime. The computer is an instrumentality of the Crime because it is used as a means of committing the Criminal offense. The computer is also likely to be a storage medium for evidence of Crime. From my training and experience, I believe that a computer used to commit a Crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the Criminal conduct was achieved; records of Internet discussions about the Crime; and other records that indicate the nature of the offense.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that

much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. Based on my training, experience, and the foregoing facts set forth herein, I believe that probable cause exists to search the address described in Attachment A, 242 Henry Street, Stanleytown, Virginia along with the curtilage surrounding that address, as described in Attachment A and to seize items described in Attachment B.

34. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A, in order to seek the items described in Attachment B.

OATH

I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

s/Daniel Bailey
Daniel Bailey, Task Force Officer
Drug Enforcement Administration

Received by reliable electronic means and sworn and attested to by telephone on this 31st day of January 2024.

C. KAILANI MEMMER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Place and Property to Be Searched

The TARGET ADDRESS is a residence located at 242 Henry Street, Stanleytown, Virginia 24168. That residence is described as a gray colored, single story, vinyl sided, single family residence. The TARGET ADDRESS contains a shed/outbuilding on the property.

This application is for a warrant to search the residences described herein and all outbuildings and vehicles on or within the curtilage of the property.

ATTACHMENT B

Property to be Seized

1. All evidence relating to violations of distribution and possession with intent to distribute controlled substances, in violation of 21 U.S.C. § 841, conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 846, and maintaining a drug-involved premises, in violation of 21 U.S.C. § 856, those violations involving Quinn HAIRSTON and their co-conspirators, including:

   a. Books, records, receipts, notes, ledgers, and other papers relating to the transporting, ordering, purchasing, and distributing of controlled substances;
   b. Photographs, including still photographs, negatives, video tapes, films, undeveloped film and the contents therein, slides, in particular photographs of co-conspirators, assets, and/or controlled substances;
   c. Address and/or telephone books, rolodex indices and any papers reflecting names, addresses, telephone numbers, pager numbers, fax machines, and/or telex numbers of co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists;
   d. Indicia of occupancy, residency, rental, and/or ownership of the premises to be searched, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase, or lease agreements, and keys.
   e. Any conversations, whether through text messages or other applications, concerning the distribution and/or possession with the intent to distribute controlled substances, bulk cash deliveries, or the laundering of drug proceeds.
   f. Lists of customers and related identifying information.
   g. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.
   h. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
   i. Any information relating to the schedule or travel of Quinn HAIRSTON or any of his known or suspected coconspirators;

j. All bank records, checks, credit card bills, account information, and other financial records; and

k. Records and information relating to the identity or location of the suspects.

l. United States currency, precious metals, jewelry, and financial instruments, including stocks and bonds;

m. Controlled substances;

n. Scales, containers, mixers, cutting tools, packaging materials, beaters, burners, and any other drug paraphernalia used in manufacturing, diluting, packaging, and distributing controlled substances;

o. Firearms and other items pertaining to the possession of firearms, including gun cases, ammunition, ammunition magazines, holsters, spare parts for firearms, firearms cleaning equipment, photographs of firearms or of persons in possession of firearms, and receipts for the purchase and/or repair of all these items;

p. Books, records, invoices, receipts, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, and cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealing, and/or expending of money;

q. Electronic equipment, such as cellular telephones (and the data contained within), computers, telex machines, facsimile machines, currency counting machines, telephone answering machines (including listening to any messages recorded on such machines), and related manuals used to generate, transfer, count, record, and/or store information. Additionally, computer software, tapes, discs, CD, DVDs, audio tapes, and the contents therein, containing the information generated by the aforementioned electronic equipment;

r. Cellular telephones, portable cellular telephones, electronic pagers, and any stored electronic communications or data contained therein.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.